(Translation)

Japanese Patent Office (JP)

UNEXAMINED PATENT PUBLICATION (A)

Patent Appln. Disclosure No.
Sho 55-20830

Int.Cl.[3] ID No. Pat.Off.Ref.
E05B 49/00 No.7606-2E

Laid-open Feb. 14, 1980
Number of Invention 1

Request for Exam.
not filed yet

Door Locking System

Pat. Appln. No. Sho 53-93356
Filed July 31, 1978
Inventor: Tani Tomoma
4-12-9 Kami-Igusa
Suginami-ku, Tokyo

Applicant: Tani Tomoma
4-12-9 Kami-Igusa
Suginami-ku, Tokyo
Applicant: Osakabe Hiroshi
1899-8 Hamura,
Hamura-cho,
Nishitama-gun,
Tokyo

Specification

1. Title of the Invention:

Door Locking System

2. Claim for Patent:

A door locking system characterized by consisting of: a detection means for detecting the insertion of a keycard for unlocking; unlocking keycode signal generating means for reading a keycode given to said keycard; locking keycode signal generating means with locking keycode signal stored therein in advance; comparing means for comparing said unlocking keycode signal and said locking keycode signal to provide an unlocking signal when they are coincident; and another detection means for determining the presence/absence of said unlocking signal provided from said comparing means when the first-mentioned detection means provides a detection output, thereby to detect

the absence of said unlocking signal.

3. Detailed Description of the Invention:

The present invention relates to an electrical door locking system and is aimed at providing such a door locking system capable of making the unlocking by a third party difficult.

According to the present invention, which is adapted to unlock in response to the comparison between the output from the unlocking keycode signal generator serving as an electrical key and the corresponding output from the locking keycode signal generator serving as an electrical lock, it is possible to detect whether or not a proper keycard is used.

Also, according to the present invention, the outputs from the above-mentioned unlocking keycode signal generator and locking keycode signal generator are compared as coinciding signals to detect the provision of the unlocking signal, making it possible to confirm proper operation without using a keycard.

Furthermore, the present invention makes it possible to arbitrarily change the memory content at the above-mentioned locking keycode signal generator and thereby to use a keycard with the keycode changed to a different one as the occasion demands, with the result that the unlocking by a third party becomes extremely difficult.

Also, according to the present invention, the storage of a plurality of locking keycode signals in the above-mentioned locking keycode signal generator makes it possible to use a plurality of keycards for a single locking device.

An embodiment of the present invention will now be described with reference to the accompanying drawings.

Referring to Fig.1 showing a door locking system of a first embodiment of the invention, the system has, as shown by dotted line blocks, unlocking keycode signal generator 1, locking keycode signal generator 2, comparator circuit 3, unlocking device 4, and power supply circuit 5. Among these, unlocking keycode signal generator 1 has, in order to generate a 16-bit unlocking keycode signal, 16 photodetector elements a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, c_1, c_2, c_3, c_4, d_1, d_2, d_3, d_4 arranged in four rows by four columns, with each of the photodetector elements connected in series with resistor R connected in turn to positive voltage power supply line 6 at its one end. Photodetector elements a_1-d_4 exhibit high level "1" output state when exposed to light rays, while they exhibit low level "0" output state when unexposed to light rays, with the result that an unlocking keycode signal is generated in the form of 16-bit binary digital signal. It will be noted here that the presence or absence of the light rays reception by photodetector elements a_1-d_4 is determined by the insertion, between light source lamp 7 and 16 photodetector elements a_1-d_4, of keycard 8 as shown in Fig.2.

To describe in greater detail unlocking keycode signal generator 1 referring to Fig.2, photodetector board 9 with 16 photodetectors a_1-d_4 arranged in four rows by four columns and light source lamp 7 are fixedly placed on the wall outside of a room or on a door, in such a manner that keycard 8 can be arbitrarily inserted into or removed from the space therebetween. Although not shown, the wall or the door has an aperture for the insertion of keycard 8 as well as a guide means for facilitating the insertion and removal of keycard 8. Keycard 8, having

addresses a_1'-d_4' arranged in four rows by four columns corresponding to the 16 photodetector elements a_1-d_4 of photodetector board 9, has light-transmissive perforations 10. As shown in Fig.3, keycard 8 has light-transmissive perforations 10 at six addresses a_1', a_4', b_2', c_3', d_1', d_3', while it intercepts the light rays at other addresses. Therefore, with the arrangement as shown in Fig.2, light rays are received only at photodetectors a_1, a_4, b_2, c_3, d_1, d_3, whose output lines exhibit "1" state, with the result that a binary digital signal [1001010000101010] corresponding to the outputs from 16 photodetector elements a_1-d_4 is provided. Switch 11 shown in Fig.2 is adapted to be turned on upon the insertion of keycard 8 into a predetermined place for unlocking thereby to initiate unlocking operation, and is connected to power supply terminal 12 as shown in Fig.1.

Locking keycode signal generator 2 has, as shown in Fig.1, input device 13 for providing locking keycode signals in the form of binary digital signals, decoder 14 constituting second input means, main memory 15 adapted to receive either the output of input device 13 or the output of decoder 14, hold circuit 16 for temporarily storing locking keycode signals read from main memory 15, read-start signal generator 17 for starting the readout at memory 15 in synchronism with the turn-on of switch 11, and line 18 for providing an end-of-read signal from memory 15.

Decoder 14 has, as shown in Fig.4, 16 photodetector elements a_1-d_4 arranged in four rows by four columns, with each of the photodetector elements connected in series with resistor R, which is connected at its one end to positive voltage power supply line

19. Respective outputs of these 16 photodetector elements a_1-d_4 are applied through buffer amplifiers 20 to buffer memory 21. Also, to power supply line 19 is connected light source lamp 22a, whose light rays are led to selected ones of phtotodetectors a_1, d_4 through keycard 8 shown in Figs.2 and 3. It will be noted that the decoder of Fig.4 employing photodetector elements a_1-d_4 is structured similarly to unlocking keycode signal generator 1 shown in Figs.1 and 2. Therefore, the insertion of keycard 8 between lamp 22a and photodiodes a_1-d_4 causes the six photodetectors a_1, a_4, b_2, c_3, d_1, d_3 to receive light rays to generate locking keycode signal [1001010000101010], which is written in buffer memory 21. Even in decoder 14, switch 22 provided to turn on in response to the insertion of keycard 8 causes power to be supplied from power supply terminal 23 to power supply circuit 24 only when keycard 8 is inserted between lamp 22a and photodetector elements a_1-d_4, thereby to cause timing pulse generator 25 coupled with power supply circuit 24 to provide write instruction for buffer memory 21 and reset signal for memory 15, which is followed by write instruction subsequent to resetting of memory 15 to result in the write-in of the output of buffer memory 21 in memory 15.

To describe comparator circuit 3 referring to Fig.1 again, it has collation circuit 26 for row a, collation circuit 27 for row b, collation circuit 28 for row c, collation circuit 29 for row d, and is structured to compare the 16-bit unlocking keycode signal generated from unlocking keycode signal generator 1 with the 16-bit locking keycode signal generated from locking keycode signal generator 2. The detailed circuit structure shown in Fig.1

for collation circuit 26 for row a applies to collation circuits 27, 28, 29 for other rows. Stated briefly, 16 collation circuits of similar structure are provided for the 16 bits. Therefore, description will be given hereunder with respect only to the collation circuit for the output of photodetector element a_1, omitting the description of other collation circuits. The output from photodetector a_1, which is the first bit of the 16-bit unlocking keycode signal, is input to first AND gate 30, to which the first bit of the 16-bit locking keycode signal is also input, with the result that AND gate 30 provides at its output line 31 output "1" when these bits are both "1." These bits are also input to second AND gate 34 through inverter 32 and 33, respectively. Therefore, second AND gate 34 provides output "1" when these bits are both "0." Stated briefly, output "1" is provided only when unlocking keycode signal coincides with locking keycode signal. Third AND gate 35 is supplied with 16 collation outputs corresponding to the 16 bits, with the result that third AND gate 35 provides output "1" only when all the 16 inputs thereto are "1." Therefore, third AND gate 35 does not provide output "1" if even 1 bit does not coincide.

Unlocking device 4 has fourth AND gate 36 supplied with the output of third AND gate 35 and the signal at end-of-memory-read signal line 18, switch circuit 27 adapted to turn on responsive to the output from fourth AND gate 36, and plunger selenoid 38 energized when switch circuit 37 is in the on state. To plunger 39 pulled in by plunger solenoid 38 is coupled protruding lock piece 40, which is biassed upward by compression coil spring 41 with respect to Fig.1. Onto door 43 adjacent to wall 42, in which

plunger 39 and lock piece 40 are embedded, is mounted engaging bar 44 movable in the left-right direction with respect to Fig.1 with recessed portion 45 to receive lock piece 40. In the state where engaging bar 44 is engated with lock piece 40 as shown in Fig.1, it is impossible to move engaging bar 44 in the left-right direction with a knob (not shown) mounted onto door 43, and to pull this out from wall 42. More definitely, door 43 is impossible to open. On the other hand, when plunger solenoid 38 is energized to move plunger 39 and lock piece 40 downward countering spring 41 with respect to Fig.1, thereby to remove lock piece 40 from recessed portion 45, engaging bar 44 is allowed to move rightward to permit door 43 to open.

Description will now be given with respect to how this door locking system is handled and operated.

To use the locking system of Fig.1, a locking keycode signal identical to the unlocking keycode signal that can be generated by keycard 8 is written in main memory 15 by the use of input device 13 or decoder 14. When input device 13 is used, the inputting is performed by a keyboard, for example, and when decoder 14 is used, the inputting is performed by reading perforations 10 of keycard 8 by the arrangement of Fig.4. This permits a binary digital signal [1001010000101010] to be stored in main memory 15 as locking keycode signal. Then, the keycard 8 is put in front of photodetector board 9 for mechanical locking operation, as shown in Fig.2. This is achieved by inserting keycard 8 into a keycard insertion slot provided on a wall adjacent to the door outside a room, for example. This turns on switch 11 to activate power supply 5 to energize circuits and

turn on lamp 7 and to read-start signal generator 17 to provide memory read-out instruction signal. The turning-on of lamp 7 results in six photodetectors a_1, a_4, b_2, c_3, d_1, d_3 receiving light rays through light emitting perforations 10 of keycard 8, with the remaining photodetectors being in non-receiving state. As a result, a digital signal [1001010000101010] is generated from unlocking keycode signal generator 1. On the other hand, locking keycode signal is generated from main memory 15. Then, comparison is performed at comparator circuit 3 between the unlocking keycode signal and the locking keycode signal. Since it is apparent that both signals are identical to each other, all the outputs corresponding to the 16 bits become "1", resulting in the output "1" from third AND gate 35. The output of third AND gate 35 is supplied to fourth AND gate 36 together with the end-of-memory read signal, which is also in the state "1," with the result that fourth AND gate 36 provides output "1." This turns on switch 37 to energize plunger solenoid 38 to permit engaging bar 44 to be inserted into key hole 46. Removing keycard 8 with engaging bar 44 kept inserted turns off switch 11 to cut off power from power supply 5, thereby to de-energize plunger solenoid 38 leaving lock piece 40 urged into recessed portion 45 of engaging bar 44 by spring 41 to achieve the locked state. While it is stated above that the removal of keycard 8 turns off the power supply to de-energize plunger solenoid 38, the removal of keycard 8 with power supply still kept on leaves all the 16 photodetector elements a_1-d_4 in light-receiving state, resulting in non-coincidence between the output from unlocking keycode signal generator 1 and the output from memory 15, turning off

switch circuit 37 and de-energizing plunger solenoid 38. In the present system, the memory content of memory 15 is of course retained even after the mechanical lock-up is achieved.

To unlock, keycard 8 is placed in parallel with photodetector board 9 as shown in Fig.2, in a manner similar to locking. This turns on switch 11 to cause unlocking keycode signal generator 1 to provide unlocking keycode signal [1001010000101010], and to cause memory 15 to provide an identical locking keycode signal, with the result that the coincidence output is provided at comparator circuit 3, which turns on switch circuit 37. As a result, plunger solenoid 38 is energized to pull out lock piece 40 from recessed portion 45 of engaging bar 44 to allow engaging bar 44 to be removed from key hole 46.

In the present system, comparator circuit 3 does not provide unlocking output "1" so far as there is no coincidence in positions of light emitting perforations 10, even if a keycard having a shape identical to keycard 8 is inserted, whether by mistake or on purpose. Since this embodiment has 16 bits, 2^{16}=65,536 different combinations are possible, making it next to impossible to prepare an unlocking keycode signal intentionally.

Since the locking keycode signal can be arbitrarily changed in this door locking system, locking keycode signal and unlocking keycode signal are changed as the occasion demands.

Fig.5 schematically shows the mode of use in which the door locking system described above is applied to a hotel.

Front desk 50 is equipped with decoder 14 and address-designating unit 51 adapted to store in memory 15 the outputs of

decoder 14 at addresses corresponding respectively to room numbers. As shown by arrow A, a guest's room number is designated by address-designating unit 51, and stored together with keycode of keycard 8 picked up from a plurality thereof. The keycard 8 is then handed to the guest as shown by arrow B. Then, the guest inserts card 8 into slot 52 of a guest room unit at his room, which activates unlocking keycode signal generator 1 and simultaneously causes an address signal to be generated, based on which the locking keycode signal stored at memory 15 is read. Then, unlocking keycode signal and the locking keycode signal are compared at comparator 3, which provides unlocking signal when there is matching.

Fig.6 shows an embodiment for judging whether a proper keycard in the present invention is used. This makes it possible to detect a hotel guest mistakenly trying to unlock another guest's room or intentionally trying to unlock with a copied keycard.

As described above, the insertion of the keycard 8 into the predetermined place turns on switch 11, to permit the keycard to be decoded into the unlocking keycode signal, and the locking keycode signal to be read from memory 15 for comparison at comparator circuit 3. However, when wrong keycard 8 is inserted, there is no unlocking signal provided. Therefore, arrangement is made to count up by counter 54 the number of times of closure of switch 11 supplied through differentiation circuit 53. Counter 54 is reset when the unlocking signal is provided by comparator circuit 3. Also, counter 54 is adapted to provide an output signal when closure of switch 11 is counted more than five times.

This output signal is provided to one of the input terminals of AND circuit 55. The output of comparator circuit 3 described above is provided through inverter 56 to the other of the input terminals of AND circuit 55. To the output terminal of AND circuit 55 is connected a light emitting diode 59 through one of the inputs to OR circuit 57 and swith 58. To the output terminal of OR circuit 57 is connected buzzer 61 through switch circuit 60. Light emitting diode 59 and buzzer 61 are provided at front desk 50, with diode 59 indicating a room number.

It follows therefore that the insertion of a wrong keycard 8 for five times or more causes counter 54 to provide an output signal to permit AND circuit 55 to ascertain the absence of the unlocking signal, thereby to turn on switches 58, 60 to energize buzzer 61 and diode 59 for light emission. Thus, it is possible for the front desk side to detect the abnormal condition at the locking device of that particular room. Based on this detection, a follow-up step can be taken. For example, the door to the room may be monitored by a television camera first for inspection of its status in response to the detection signal.

In the above circuit arrangement, AND circuit 55 and inverter 56 can be omitted if counter 54 is adapted to provide output upon two-time closures of switch 11. The provision, adjacently to the insertion slot for keycard 8, of a light emitting diode adapted to be energized simultaneously with the above-mentioned light emitting diode 59 will permit the ascertaining by the user.

As described above, while the present system makes it possible to immediately unlock in response to the use of a proper

keycard, the use of a wrong keycard is detected without leading to unlocking, with the result that countermeasures and follow-up steps can be taken swiftly. This is particularly advantageous in such an environment where a plurality of locking devices are under centralized control, as in hotels and other buildings having a number of offices. The use of the counter to accomodate a certain number of incorrect insertion is suited for day-to-day use.

Fig.7 shows an arrangement for enabling the monitoring of the status of the door locking system without using the keycard employed in the present invention. Memory 15 stores a testing keycode signal with all the 16 bits consisting of "1." This signal means that all the addresses a_1'-d_4' of keycard 8 have light transmissive apertures 10, which is unsuited for unlocking through the use of keycard 8. Therefore, this signal is excluded from locking keycode signals. Reference numeral 62 denotes a decision circuit for testing keycode signal; and 63, a switch circuit controlled by the output signal of decision circuit 62. Reference numerals 64 and 65 denote AND circuits connected respectively to the output side of comparator 3; and 66, an inverter. Reference numeral 67 denotes a light emitting diode turned on and off by switch circuit 68. This switch circuit 68 is turned on and off in synchronism with the output signal from oscillator 70 supplied through OR circuit 69. It is on-off controlled also by the presence/absence of the output signal from AND circuit 65.

In this circuit arrangement, the monitoring of the status is performed by reading from memory 15 the testing keycode signal

and supplying it to readout comparison circuit 3. Decision circuit 62 recognizes the presence of the testing keycode signal, and its output signal activates switch circuit 63 to turn on power supply. At unlocking keycode signal generator 1, light source lamps 7 is turned on as shown in Fig.1 and Fig.2. Because of the absence of the insertion of keycard 8, all the photodetector elements a_1-d_4 are irradiated to provide the 16-bit keycode signal with all the bits constituted by "1." Thus, comparison output 3 provides an unlocking signal. However, this unlocking signal is not provided at the output of AND circuit 64 and consequently does not energize unlocking device 4, because of the output of decision circuit 62 supplied to AND circuit 64 through inverter 66. On the other hand, the unlocking signal supplied to AND circuit 65 provides the output from AND circuit 64 to which the output from decision circuit 62 is also applied, thereby to turn on switch circuit 68 and to keep light emitting diode 67 energized.

If light source lamp 7 failed to be turned on because of a certain trouble, or if any of photodetector elements a_1-d_4 failed to function even after exposure to light rays, or if the light rays were intercepted by dust, no coincidence is obtained in the result of comparison by comparator circuit 3. Under such state, the unlocking signal is not provided and no output is provided at the output side of AND circuit 65. Switch circuit 68 is turned on and off in response to the oscillation frequency of oscillator 70. Accordingly, light emitting diode 67 is turned off and on at the interval corresponding to the above frequency. In other words, the on-off operation of light emitting diode 67 indicates

the occurrence of trouble, while its continued light emission indicates normal operation.

Thus, it is possible to ascertain, without using a keycard, whether the door locking system functions properly or not. This permits remote control. The use of this system is suited for centralized control of a plurality of locking devices and can be applied not only to hotels but to buildings having a number of offices.

In the case of centralized control, light emitting sources are arranged at a display panel corresponding respectively to the locking devices, to which the identification numbers, names and the like of the locking devices are respectively made to correspond, thereby to selectively enable the simultaneous or separate testing and to permit the ascertaining through the on and off states of the light emitting sources on the display panel.

While light emitting sources have been used in the foregoing for displaying the test results, any means for indicating the results of the ascertaining such as sound generating means can be used.

Next, the preparation of a keycard on each accasion of its use will be described referring principally to Fig.8, Fig.9 and Fig.10.

Keycards 8, before the perforations are formed, are kept with identification numbers assigned corresponding to the serial numbers of the locking devices. In a hotel, for example, keycards 8 are kept at the front desk with room numbers given and with light emissive perforations not formed yet. Locking keycode

signal generator 2 has, as shown in the cross-sectional view of Fig.8 and the plan view of Fig.9, a light transmissive perforation forming device. There are 16 plungers 71_1-71_{16} and solenoids 72_1-72_{16} arranged in 4 rows by 4 columns. Facing these elements, are formed 16 receiving holes 73_1-73_{16}. Thus, if selenoid 72_1, for example, is excited with keycard 8 inserted, plunger 71_1 penetrates into receiving hole 73_1 as shown by dotted lines. This results in the formation of light transmissive perforation 10 at address a_1' of keycard 8 shown in Fig.3.

Reference numeral 74 denotes a reading device for reading out the room number given to keycard 8 and for converting it to an address signal. Reference numerals 75_1-75_{16} denote light emitting diodes arranged on the sides of receiving holes 73_1-73_{16}, and 76_1-76_{16} denote phototransistors arranged on the sides of receiving hole 73_1-73_{16} facing the light emitting diodes, so as to determine whether plungers 71_1-71_{16} have penetrated through receiving holes 73_1-73_{16}.

In Fig.10, reference numeral 77 denotes a randon number signal generator circuit adapted to provide 16-bit binary digital signal; and 78, a hold circuit arranged to provide unpredictable binary digital signals, with random number signal generator circuit energized in response to instruction signal from timing pulse generator circuit 25 upon closure of switch 22 by the insertion of keycard 8. Reference numerals 79_1-79_{16} denote switch circuits; 80 and 81, buffer memories; 82, comparator circuit; 83 and 84, AND circuits; 85 and 86, switch circuits; 87 and 88, light emitting diodes adapted to provide green- and red-colored light rays; and 89, a delay circuit.

In response to the above-mentioned binary digital signal generated at random, switch circuits 79_1-79_{16} are on-off controlled, thereby to selectively excite solenoids 72_1-72_{16} to cause plungers 71_1-71_{16} to selectively penetrate through receiving holes 73_1-73_{16}. Thus, light-transmissive perforations 10 are formed at addresses of keycard 8 corresponding to the above binary digital signal. This perforation formation is detected by phototransistors 76_1-76_{16} responsive to whether light rays irradiated from light emitting diodes 75_1-75_{16} are intercepted by plungers 71_1-71_{16}, with the detection output signal stored at buffer memory 80. The output signals from the above-mentioned hold circuit 78 and buffer memory 80 are provided to comparator circuit 82 for determining the coincidence between the two. Since the formation of the light-transmissive perforations in keycards 8 takes time, the read instruction from buffer memory 80 is supplied through delay circuit 89. The output from comparator circuit 82 writes the binary digital signal from hold circuit 78, in buffer memory 81, thereby to control the writing/reading of memory 15 shown in Fig.1 and Fig.4.

This control writes in memory 15 as the locking keycode signal the binary digital signal supplied from hold circuit 78 through buffer memory 81 in response to AND circuit 83 adapted to take logical product of the post-delay representing signal set at delay circuit 89, the coincidence-representing signal from comparator 82 and the end-of-read signal. The address of write in at memory 15 is designated by the address signal from the read out device. Also, with switch circuit 85 turned on, the light emitting diode is energized to emit green-colored light rays

indicating normal operation.

If the signal indicating the coincidence at the comparison result is not provided, the logical product from AND circuit 84 turns on switch circuit 86, thereby to energize light emitting diode 88 to provide red-colored light rays indicating abnormality. On the other hand, because of the output from AND circuit 83, the binary digital signal from hold circuit 78 is not written in memory 15.

Thus, a fresh locking keycode signal is written in memory 15. On each such occasion, in keycard 8 is written the above-mentioned keycode signal. Accordingly, it is possible to unlock with this keycard 8 in a manner described referring to Fig.1. This keycard 8 can be destroyed once it has been used and, if a fresh locking keycode signal is again selected with a fresh keycard 8, unlocking by other keycards such as a previously used one, for example, cannot be achieved.

While the above-mentioned binary digital signal is provided by random number signal generator 77, it can be replaced by alternative structures including a keyboard adapted to provide an arbitrary binary digital signal on each occasion. Also, the formation of light-transmissive perforations in keycard 8 can be achieved not only by the plunger-based mechanical arrangement but also by a chemical procedure in which, for example, a photosensitive material-coated keycard is exposed to light rays for the light transmissive hole formation. Furthermore, while the keycards are given identification numbers in advance to provide read address designation signal, an alternative method may be used, in which such numbers are given to keycards by an ordinary

printer based on the address designation.

If a newly set unlocking keycode signal turned out to be the one which had been used earlier, such signal should be excluded. This is because the unlocking can be made by the use of such a previously used keycard. In the arrangement of Fig.10, therefore, such inconvenience is eliminated by the use of a circuit sturucture as shown by imaginary lines.

That is arranged to read the binary digital signal obtained at random number signal generator 77 from buffer memory 81 and to supply it into comparator circuit 90. On the other hand, the locking keycode signal written in memory 15 with addresses designated by reading device 74 is read out into comparator circuit 90 for comparison between the two and, if there is no coincidence, power is supplied from power supply circuit 91 to solenoids 72_1-72_{16} and switch circuits 79_1-79_{16}. If the comparison result shows coincidence, power supply circuit 91 stops the supply of power, thereby to generate again a fresh binary digital signal from random number signal generator circuit 77 through timing pulse generator circuit 25.

This completely eliminates the risk of unlocking by such a previously used keycard. The comparison with locking keycode signals of all other locking devices can also be performed. Furthermore, the comparison with those of locking devices of a certain region can also be performed. This is made possible by designating addresses. Thus, unlocking of two or more locking devices with a single keycard at all the locations or at a certain region of a building is made impossible, with the result that a door locking system with very high security is provided.

In the present invention, two or more keycards may be used in some cases for an unlocking device. In a hotel, for example, where a room is shared by two guests who hold keycards respectively, their stay may be in such a manner that the two stay on the first day and one of them stays on into the second day. In such a case, the use of identical keycards by the two guests permits one of them to unlock the door on the second day after the other of them left with his own keycard. The door can be unlocked also by a person who has obtained one of the keycards that was inadvertently lost by the guest.

While the keycard including the other of the keycards held by the other of the guests can be changed in such a case to fresh ones on each occasion, that would be troublesome, involving the risk of being unlocked in the above-mentioned manner unless the change is delayed.

Therefore, memory 15 is arranged to have a plurality of addresses for each locking device as shown in Fig.11. Reference numerals 1a-1z respectively denote unlocking keycode signal generators; 3a-3z, comparator circuits, respectively; 4a-4z, unlocking devices, respectively; with memory 15 having three addresses am1, am2, am3, ···, mm1, mm2, mm3, ···, zm1, zm2, zm3 corresponding respectively thereto. Reference numerals 92 and 93 respectively denote address circuits; 94, address signal generating circuit; and as1, as2, as3, ···, ms1, ms2, ms3, ···, zs1, zs2, zs3, address switches, respectively.

When two guests share room a having unlocking device 4a, mutually different keycode signals are stored at addresses am1 and am2, respectively. This is done by manipulating address

switches as1 and as2 to designate these addresses. Description of locking keycode signal generator 4 will be omitted because it is identical to the one given above. Also, for address designation, alternative methods by reading the numbers out of the keycards can be employed, in place of the use of switches as in the above embodiment. Address am3 is for use by a master keycard.

To unlock, prescribed keycard 8 causes unlocking keycode signal generator to provide a keycode signal to comparator circuit 3a, while the address signal of room a is given to address circuit 92. Then, address circuit 92 reads locking keycode signals of addresses am1, am2, and am3 sequentially to provide them to comparator circuit 3a. In the case of a master keycard, the matching is achieved with the locking keycode signal from address am3. The keycard 8 is in coincidence with the locking keycode signal of either address am1 or am2. If the use of the keycard 8 corresponding to address am1 is to be discontinued, its locking keycode signal may be replaced with a new one or erased. This permits the continued use, without any change, of the other of the keycards 8 corresponding to address am2.

While various modes of operation have been described above with respect to the present invention, enabling the objects and advantageous effects thereof to be achieved even with a single locking device, further advantageous effects can be achieved in the centralized control of a plurality of locking devices performed at the front desk of a hotel or at the guard's office of a building as shown in Fig.12.

More specifically, in a building, which has locking mechanisms corresponding to rooms 95_{11}-95_{1z} in the first floor; locking mechanisms corresponding to rooms 95_{21}-95_{2z} in the second floor; ···; and locking mechanisms corresponding to rooms 95_{n1}-95_{nz} in the n-th floor, centralized control device 96 including a memory device for applying the above-mentioned various modes of the present invention to each locking mechanism is placed at the front desk, the guard's office and the like. These components are linked by a common wiring to permit each control by a time devision-based control. Reference numeral 97 denotes a decoding device or a setting device for setting keycode signals.

Similarly, the above-mentioned time devision-based control can be applied through the single wiring to the detection of the incorrect operation of each locking device, and to the checking of whether the operation is proper or not, and the like, by the use of conventional well-known means.

The time division-based control satisfies any function of the presnt invention with the use of the minimum single wiring, making the present system very preferable in terms of system construction and manufacturing cost.

While the above embodiment of the invention utilizes transmission of light rays, these rays may be radiation or the like. Similarly, a magnetic keycard capable of forming keycode signals may be used. In addition, keycode signals may be formed by a mechanism adapted to mechanically detect the unevenness formed on the keycard.

As has been described, since the rewriting of locking keycode signal is made possible according to the invention, not

only the need for changing electrical and mechanical locking device is virtually eliminated even when the keycard is inadvertently lost or improperly used by a third party, but also the use of wrong keycards can be detected.

Furthermore, the operation status of the locking device can be ascertained without using the keycard.

Also, the change of a locking keycode signal can be achieved swiftly, providing great convenience to operation. Furthermore, the post-change new locking keycode signal can be set only after it is ascertained that there is not any possibility of being unlocked.

4. Brief Description of Drawings:

Fig.1 shows a circuit diagram of a door locking system associated with respective embodiments of the present invention; Fig.2 shows a perspective view of an unlocking keycode signal generator; Fig.3 shows a plan view of a keycard; Fig.4 shows a circuit diagram of a decoder; Fig.5 shows a perspective view of the mode of use in which the door locking system of the present invention is applied to a hotel; Fig.6 shows in blocks an embodiment of the invention for ascertaining whether the mode of use in the invention is correct or not; Fig.7 shows in blocks an embodiment for ascertaining the operation of the locking device in the invention; Fig.8 shows a cross sectional view of an embodiment of a device for preparing a fresh keycard in the present invention; Fig.9 shows a plan view thereof; Fig.10 shows a block diagram thereof; Fig.11 shows in blocks an embodiment in which a plurality of keycards are used for a locking device in the present invention; and Fig.12 shows in blocks an embodiment

in which a plurality of locking devices are put under centralized control with the present invention described above generalized.

1···unlocking keycode signal generator; 2···locking keycode signal generator; 3···comparator circuit; 4···locking device; 8···keycard; 14···decoder; 15···memory; 59···light emitting diode.

Tani Tomoma
Osakabe Hiroshi, Applicants

(Legends in the drawings other than those listed above)

[Fig.1]

5···power supply circuit; 13···input device; 16···hold circuit; 38···plunger solenoid

[Fig.4]

21···buffer memory; 24···power supply circuit; 25···timing pulse generator

[Fig.6]

5···power supply circuit; 53···differentiating circuit; 54···counter

[Fig.7]

5···power supply circuit; 62···decision circuit; 70···oscillator circuit

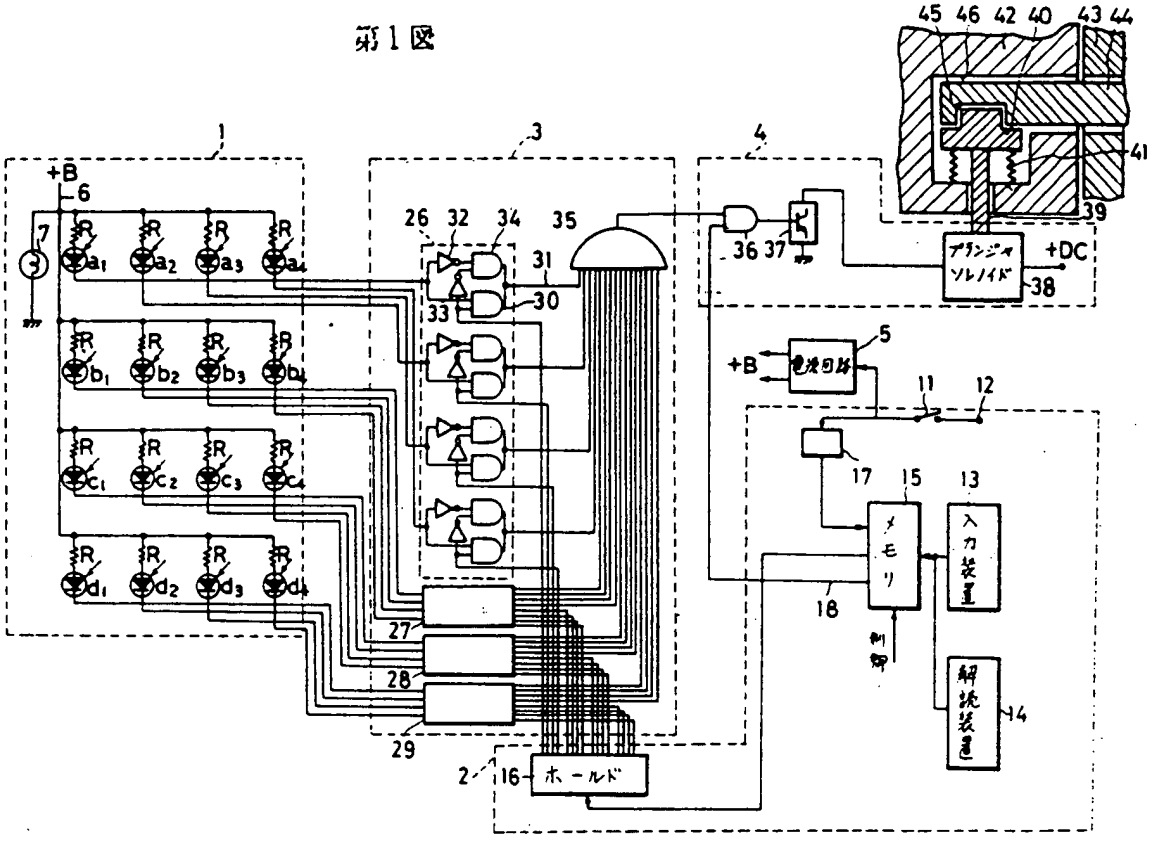
[Fig.10]

25···timing pulse generator; 74···read-out device; 77···random number signal generator; 78···hold circuit; 80,81···buffer memory; 82···comparator

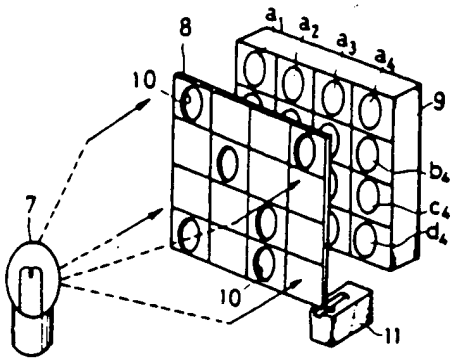
[Fig.11]

92···address circuit; 93···address circuit; 94···address signal generator circuit

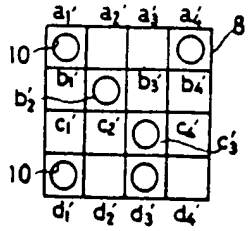
第1図


+B
6
7
R
a1
a2
a3
a4
b1
b2
b3
b4
c1
c2
c3
c4
d1
d2
d3
d4
1
3
4
26
32
34
35
31
30
33
27
28
29
2
16
ホールド
36
37
45
46
42
40
43
44
41
39
アクシュエータ
ソレノイド
+DC
38
5
電源回路
11
12
17
15
13
メモリ
入力装置
18
制御
解読装置
14

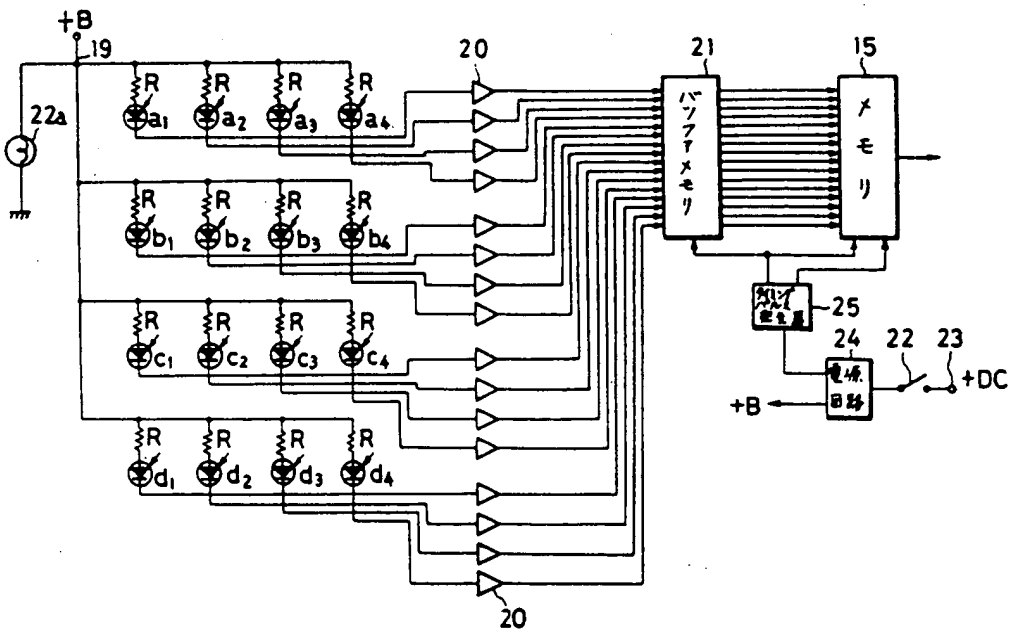
第2図



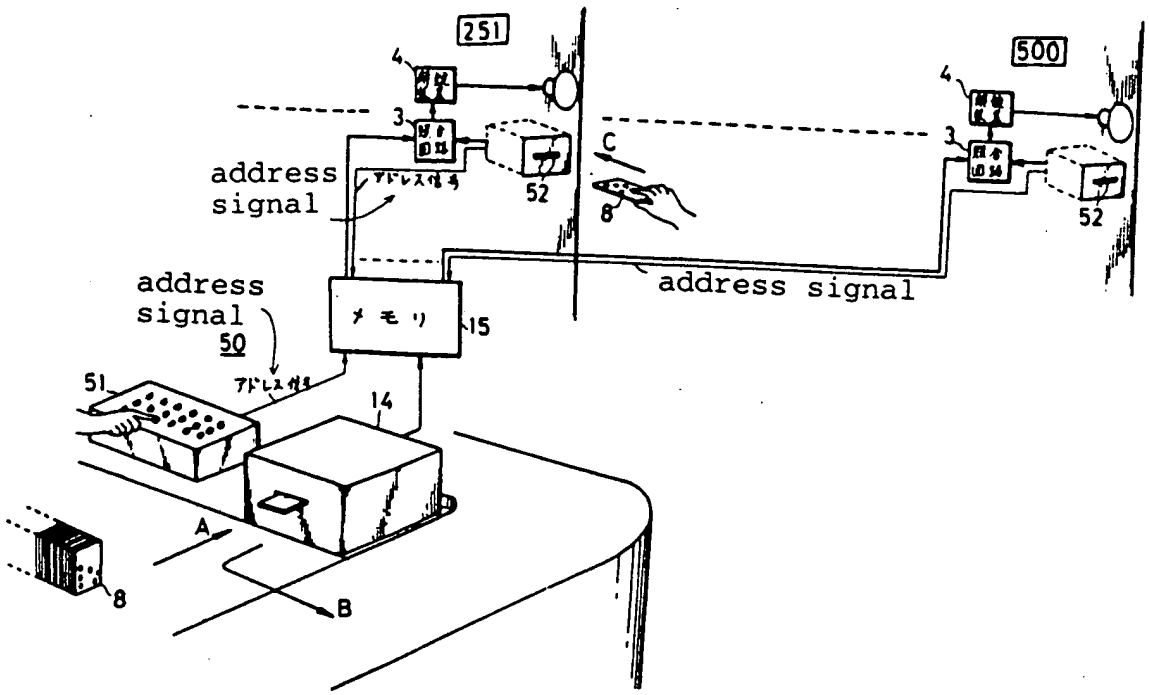
第3図



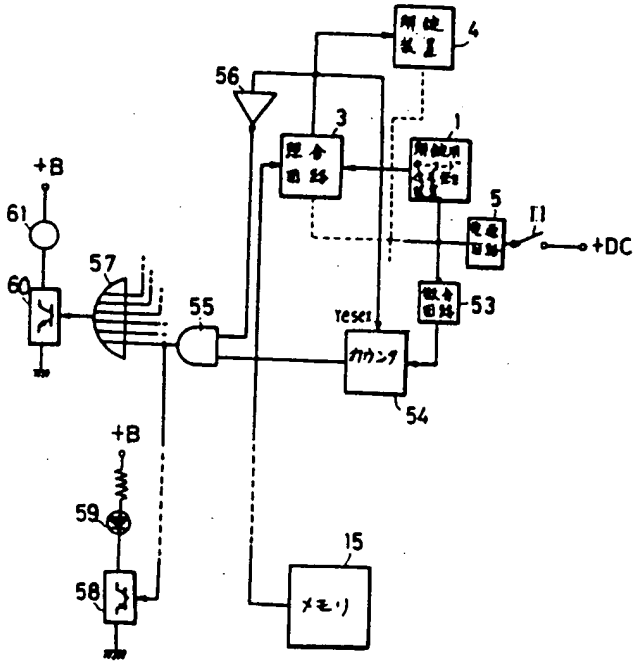
第4図



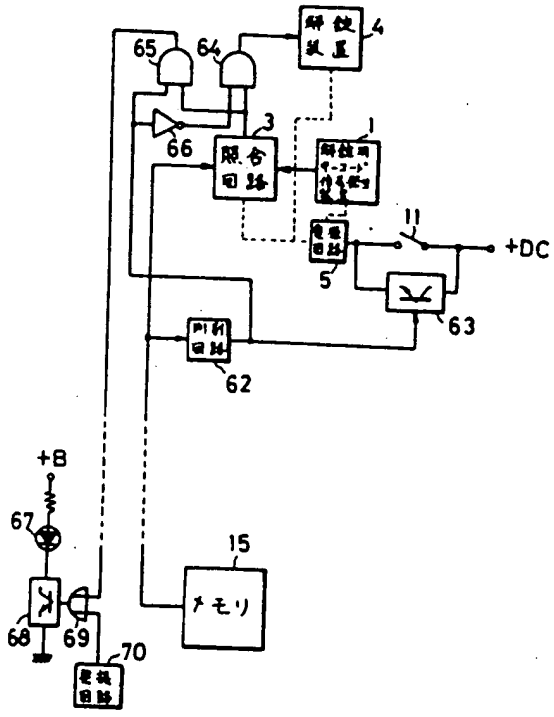
第5図


251
500
address signal
address signal
address signal
50
メモリ
15
14
51
52
3
4
C
8
A
B

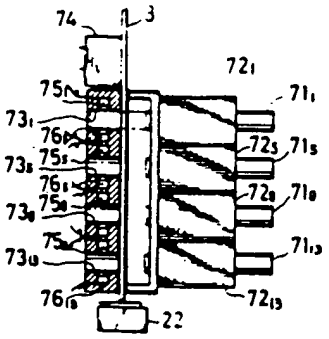
第6図


+B
61
60
57
56
55
3
1
5
11
+DC
53
54
reset
カウンタ
59
58
15
メモリ
4

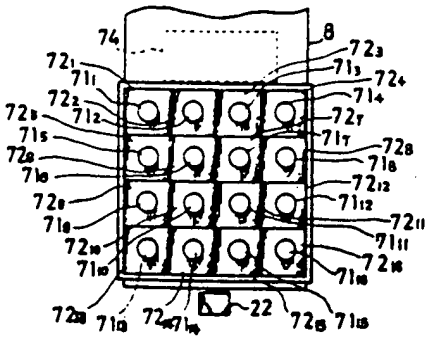
第7図


65
64
66
3
1
5
11
+DC
63
62
+B
67
68
69
70
15
メモリ
4

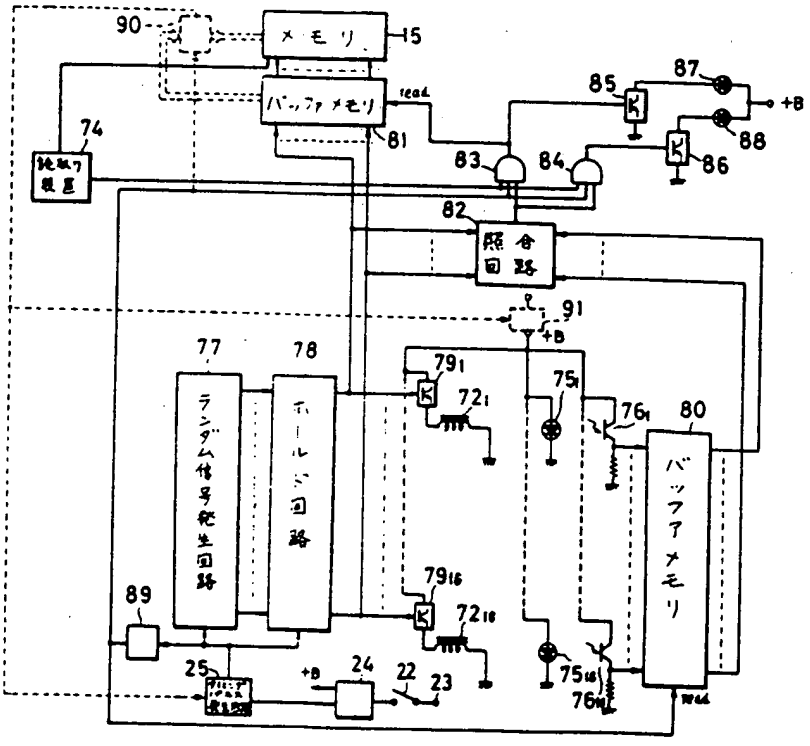
第8図


74
3
72₁
75₁
71₁
73₁
76₁
72₅
71₅
73₅
75₅
76₅
72₉
71₉
73₉
75₉
71₁₃
73₁₃
76₁₃
72₁₃
22

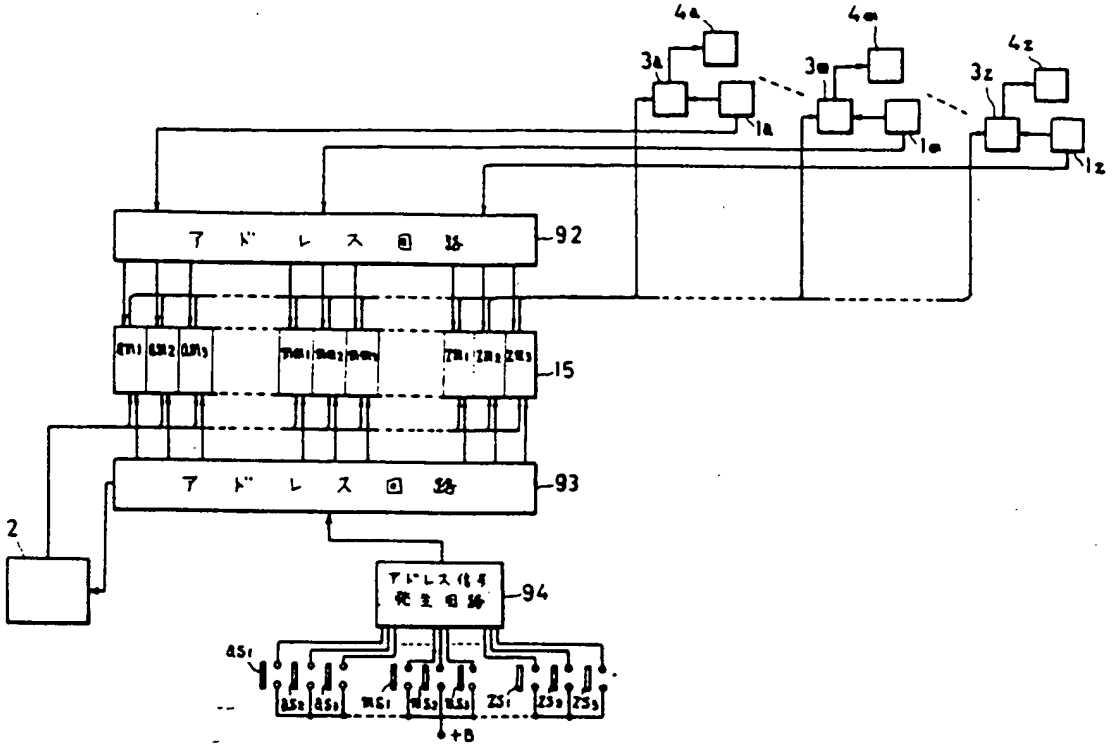
第9図


74
8
72₁
71₁
72₂
71₂
72₃
71₃
72₄
71₄
72₅
71₅
72₆
71₆
72₇
71₇
72₈
71₈
72₉
71₉
72₁₀
71₁₀
72₁₁
71₁₁
72₁₂
71₁₂
72₁₃
71₁₃
72₁₄
71₁₄
72₁₅
71₁₅
72₁₆
71₁₆
22

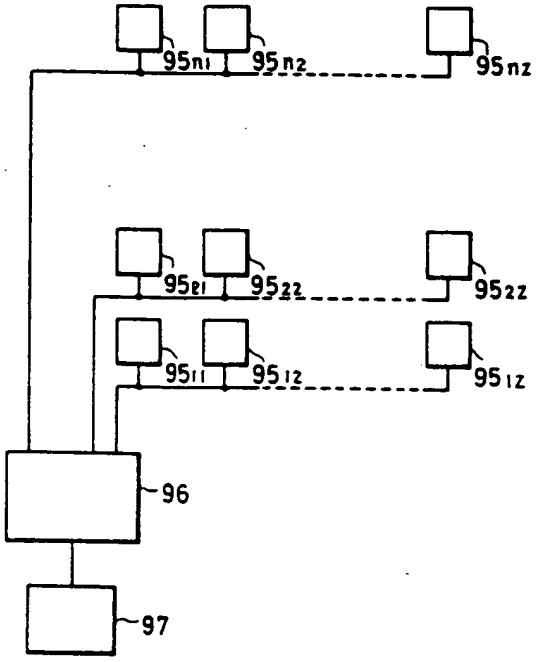
第10図


90
メモリ
15
バッファメモリ
read
81
74
85
87
+B
88
86
83
84
82
照合回路
91
+B
77
78
79₁
75₁
72₁
76₁
80
ランダム信号発生回路
ホールド回路
バッファメモリ
79₁₆
72₁₆
75₁₆
76₁₆
89
25
+B
24
22
23
W44

第11図


4a
4m
4z
3a
3m
3z
1a
1m
1z
アドレス回路
92
15
アドレス回路
93
2
アドレス信号発生回路
94
+B

第12図


95n1
95n2
95nz
95z1
95z2
95zz
95i1
95i2
95iz
96
97